We have reviewed the information from your security brAin box: Sample Report-1c458fe9

The reporting period was: 1st January 2020 until 31st January 2020

Powered by Amplify Intelligence

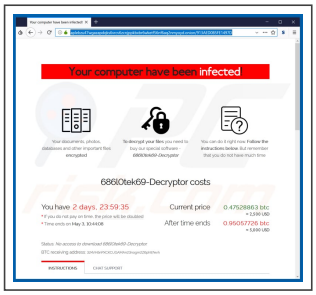
Your January 2020 Snapshot

Tracking 58.4 million threats globally over the last 3 months.

Total Devices	AntiVirus updated	Operating Systems updated	Unique External Hosts*	Suspicious activity**	High Risk Internal systems	Cloud Usage	Connections Observed
30 ↑ 3	11 ↓ 2	13 ↓ 5	12.7K ↑ 265	887 ↓ 192	10 ↓ 2	10 ↓ 6	2.2M ↑ 10%

Threat Feed this month

There has been an increase in attacks using a ransomware-type program called Sodinokibi. The program encrypts files stored on victims' computers -- preventing people from accessing the files until a ransom is paid. Recent attacks, affecting companies such as Travelex, are not only encrypting the data, but also steal the data beforehand. If victims don't pay the ransom, then the attackers slowly start leaking the data to the public until the attackers are paid off.



Security Awareness

Advice for staff impacted

On 22 January 2020, Microsoft announced that it had suffered a data breach resulting in the exposure of a customer support database containing 250 million records. Although Microsoft hasn't found evidence of an unauthorised user accessing the database, attack groups may take advantage of this breach, contacting you to tell you that your information was exposed and to reset your credentials. Do not respond to random **Microsoft Support** emails asking you to reset or verify your credentials and be wary of any suspicious links contained in these emails.

Highlighted Risk Events

Issues identified in the table below are ranked by a Risk score out of 10 (10 is very bad, 0 is nothing identified).

IP Address	Name (if known)	MAC Address	Score	Threat Impacting Systems.	Actions
10.10.0.22	desktop-4e39.local	9457309ca59f	10.0	OS End Of Life Detection. The Operating System on the remote host has reached the end of life and should not be used anymore.	Replace this system with one that is supported and secure.
10.10.0.12	desktop-0a67.local	f44d5c6dc325	9.3	This host is missing a critical security update according to Microsoft Bulletin MS17-010. Successful exploitation will allow remote attackers to gain the ability to execute code on the target server, also could lead to information disclosure from the server.	Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory.
10.10.0.21	server-81f9.local	408d289eb1df	6.3	This has connected with 20 external machines that have been identified as bad. The total number of bad interactions is 330.	Recommend running an alternative antivirus software on the identified systems, such as MalwareBytes.

This Month's Security Homework - Time to upgrade Windows 7 Server 2008!

On 14 January 2020, Microsoft stopped providing security updates and technical support for Windows 7, Server 2008 and Server 2008 R2. This means that those devices are no longer protected from the latest threats. Therefore, in order to ensure you continue to receive the latest security updates, upgrade your Windows 7 devices to Windows 10, and your Server 2008 devices to either Azure cloud services or Windows Server 2016 or 2019. If you have a Windows 7 device that is less than three years old, you should be able to upgrade that device to Windows 10 with no issues. However, hardware that is older than three years will likely not be able to support Windows 10 and will, therefore, need to be replaced. For Server 2008/Server 2008 R2, Microsoft recommends that users transition their servers to Azure cloud services or upgrade their servers to Server 2016 or 2019. However, in order to upgrade to Server 2016 or 2019, you will need to upgrade to Server 2012 first. Windows 7 users should visit https://support.microsoft.com/en-au/help/4057281/windows-7-support-ended-on-january-14-2020 for further information and assistance with upgrading to Windows 10 - Server 2008 and Server 2008 R2. Visit https://www.microsoft.com/en-au/cloud-platform/windows-server-2008 for further information and assistance with upgrading in the cloud.

Amplify Intelligence

** The number of unique external hosts or machines that internal systems or devices have connected with.*
*** These are detected through our Global Threat Intelligence network and unique Acuity AI platform.*

Please visit our website at https://www.amplifyintelligence.com for more information on keeping yourself safe.